

## UNITED STATES DISTRICT COURT

for the  
Middle District of North Carolina

In the Matter of the Search of  
(Briefly describe the property to be searched  
or identify the person by name and address)

Case No. 1:20MJ186-1

Christopher Hall's HP laptop computer, model number  
440 G3, serial number 5CD626JP8

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

Christopher Hall's HP laptop computer, model number 440 G3, serial number 5CD626JP8, which is stored at Gate City Charter Academy, a charter school in Guilford County, located at 123 Flemingfield Road, Greensboro, North Carolina, located in the Middle District of North Carolina, there is now concealed (identify the person or describe the property to be seized):

Evidence of, instrumentalities used in committing, and fruits of the crimes of 18 U.S.C. § 2252A(a)(5)(B) and § 2252A(a)(2)(A) as further described in Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;  
☒ contraband, fruits of crime, or other items illegally possessed;  
☒ property designed for use, intended for use, or used in committing a crime;  
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252A(a)(5)(B)	Possession of Child Pornography
18 U.S.C. § 2252A(a)(2)(A)	Distribution of Child Pornography

The application is based on these facts:

Please see the attached Affidavit.

- ☒ Continued on the attached sheet.  
☐ Delayed notice of \_\_\_\_\_ days (give exact ending date if more than 30 days: \_\_\_\_\_) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

/s/ Emily R. Keller

Applicant's signature

Emily R. Keller, SPECIAL AGENT, FBI

Printed name and title

On this day, the applicant appeared before me via reliable electronic means, that is by telephone, was placed under oath, and attested to the contents of this Application for a search warrant in accordance with the requirements of Fed. R. Crim. P. 4.1.

Date: 06/30/2020 3:00p.m.

City and state: Durham, North Carolina



Judge's signature

Joe L. Webster, U.S. Magistrate Judge

Printed name and title

**AFFIDAVIT IN SUPPORT OF**  
**AN APPLICATION FOR A SEARCH WARRANT**

I, Emily R. Keller, a Special Agent with the Federal Bureau of Investigation, being duly sworn, depose and state as follows:

**INTRODUCTION**

1. This affidavit is being submitted in support of an application for a search warrant for an electronic device ("SUBJECT'S WORK LAPTOP"), more specifically described in Attachment A of this affidavit for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§2252A(a)(2)(A) and 2252A(a)(5)(B) which are more specifically described in Attachment B of this affidavit.

2. The statements in this Affidavit are based in part on information provided by other law enforcement officers and on my investigation of this matter. Since this Affidavit is being submitted for the limited purpose of securing a search warrant, I have not included each and every fact known to me concerning this investigation. I have set forth only the facts that I believe are necessary to establish probable cause to believe that contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B) are presently located in the SUBJECT'S WORK LAPTOP.

### **AFFIANT BACKGROUND**

3. I am a Special Agent of the Federal Bureau of Investigation ("FBI"), and have been since October of 2019. My initial training consisted of an eighteen-week FBI new agent course during which I received instruction on various aspects of federal investigations, ranging from economic espionage and child pornography, to kidnapping and computer intrusions. In addition, I have earned both a Bachelor of Arts in International Studies and a Master of Public and International Affairs. I am currently assigned to the Charlotte Division and stationed at the Greensboro Resident Agency. As I am new to investigations involving child exploitation and child pornography, FBI Special Agent Tara S. Thomas, who has investigated child pornography cases for more than eight years, assisted me with drafting this Affidavit. Prior to becoming a Special Agent of the FBI, I worked as a Staff Operations Specialist, investigative analyst, for the FBI for over four years. I have supported numerous FBI investigations through investigative research and analysis, to include investigations of cybercrime. I am familiar with, and have employed, investigative techniques used in these investigations, such as analysis of Internet Protocol addresses and Internet Service Provider records. Moreover, I am a federal law enforcement officer who is engaged in enforcing the criminal

laws, including 18 U.S.C. § 2252A, and I am authorized by law to request a search warrant. As a Special Agent, I am authorized to investigate violations of laws and to execute warrants issued under the authority of the United States.

#### STATUTORY AUTHORITY

4. As noted above, this investigation concerns alleged violations of the following:

a. 18 U.S.C. § 2252A(a)(2)(A) prohibits a person from knowingly receiving or distributing child pornography, as defined in 18 U.S.C. § 2256(8), using any means and facility of interstate and foreign commerce, that has been mailed, or that has been shipped and transported in and affecting interstate and foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(1).

b. 18 U.S.C. § 2252A(a)(5)(B) prohibits a person from knowingly possessing or knowingly accessing with intent to view any material that contains an image of child pornography, as defined in 18 U.S.C. § 2256(8), that has been mailed, shipped or transported using any means or facility of interstate or foreign commerce or in or affecting

interstate or foreign commerce by any means, including by computer, or that was produced using materials that have been mailed or shipped or transported in or affecting interstate or foreign commerce by any means, including by computer. Attempts and conspiracies are also violations of this statute. 18 U.S.C. § 2252A(b)(2).

### DEFINITIONS

5. As The following definitions apply to this Affidavit and Attachment B:

a. "Chat," as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

b. "Child erotica," as used herein, means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors engaging in sexually explicit conduct.

c. "Child pornography," as defined in 18 U.S.C. § 2256(8), is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical or other means, of sexually explicit conduct, where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

d. "Computer," as used herein, refers to "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device" and includes smartphones, other mobile phones, and other mobile devices. *See* 18 U.S.C. § 1030(e)(1).

e. "Computer hardware," as used herein, consists of all equipment that can receive, capture, collect, analyze, create, display,

convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, "thumb," "jump," or "flash" drives, which are small devices that are plugged into a port on the computer, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

f. "Computer passwords and data security devices," as used herein, consist of information or items designed to restrict access to or hide computer software, documentation, or data. Data security devices may consist of hardware, software, or other programming code. A password (a string of alpha-numeric characters) usually operates what might be termed a digital key to "unlock" particular data security devices. Data security hardware may include encryption devices, chips, and circuit boards. Data security software may include programming

code that creates “test” keys or “hot” keys, which perform certain pre-set security functions when touched. Data security software or code may also encrypt, compress, hide, or “booby-trap” protected data to make it inaccessible or unusable, as well as reverse the process to restore it.

g. “Geolocated,” as used herein, refers to the identification of the geographical location of (a person or device) by means of digital information processed via the Internet.

h. “Hashtag,” as used herein, refers to a word or phrase preceded by a hash or pound sign (#), which is used to identify messages or groups on a specific topic.

i. A “Hash value” is a unique multi-character number that is associated with a computer file. Some computer scientists compare a hash value to an electronic fingerprint in that each file has a unique hash value. Any identical copy of the file will have exactly the same hash value as the original, but any alteration of the file, including even a change of one or two pixels, would result in a different hash value. Hash values represent large amounts of data as much smaller numeric values, so they are used with digital signatures.





j. “Internet Service Providers” (“ISPs”), as used herein, are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, email, remote storage, and co-location of computers and other communications equipment.

k. An “Internet Protocol address” or “IP address,” as used herein, refers to a unique numeric or alphanumeric string used by a computer or other digital device to access the Internet. Every computer or device accessing the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer or device may be directed properly from its source to its destination. Most Internet Service Providers (“ISPs”) control a range of IP addresses. IP addresses can be “dynamic,” meaning that the ISP assigns a different unique number to a computer or device every time it accesses the Internet. IP addresses might also be “static,” if an ISP assigns a user’s computer a particular IP address that is used each time the computer accesses the Internet. ISPs typically maintain logs of the subscribers to whom IP addresses are assigned on particular dates and times.

1. The "Internet" is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

m. "Minor," as defined in 18 U.S.C. § 2256(1), refers to any person under the age of eighteen years.

n. "Mobile application" or "chat application," as used herein, are small, specialized programs downloaded onto mobile devices, computers and other digital devices that enable users to perform a variety of functions, including engaging in online chat and sending or receiving images and videos.

o. "Records," "documents," and "materials," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade, photographic, mechanical, electrical, electronic, or magnetic form.

p. "Remote computing service", as defined in 18 U.S.C. § 2711(2), is the provision to the public of computer storage or processing services by means of an electronic communications system.

q. “Sexually explicit conduct,” as defined in 18 U.S.C. § 2256(2), means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the anus, genitals, or pubic area of any person.

r. A “storage medium” is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, “thumb,” “jump,” or “flash” drives, CD-ROMs, and other magnetic or optical media.

s. “Visual depiction,” as defined in 18 U.S.C. § 2256(5), includes undeveloped film and videotape, data stored on computer disc or other electronic means which is capable of conversion into a visual image, and data which is capable of conversion into a visual image that has been transmitted by any means, whether or not stored in a permanent format.

### **PROBABLE CAUSE**

9. On April 15, 2020, an FBI undercover agent, known as an “Online Covert Employee” (OCE) utilized the Kik messenger application to investigate potential pedophiles online. Kik is a mobile application designed for chatting

or messaging. The OCE interacted with an individual using the Kik username, "chris32033", subsequently identified as Christopher HALL through investigative means detailed below, on two different platforms. Kik user "chris32033" was interacting in a Kik chat group utilized by individuals to discuss and trade child sexual exploitation material. Kik user "chris32033" identified himself as a 35 year old male from the United States while he was in the chat group. After Kik user "chris32033" informed another member in the chat group that he had sexual intercourse with his son who "chris32033" purported to be 13 years old, the OCE sent a private message to user "chris32033" to begin chatting with user "chris32033" as further described below.

10. On April 15, 2020, the OCE entered Kik chat group #dadboysangel. At this time, the OCE noticed "chris32033" informed another chat group member that "chris32033" had sexual intercourse with his son. At 1:30 p.m., the OCE sent a private message to "chris32033" and began chatting with "chris32033" to ascertain whether he had access to children, and if so, whether he was sexually abusing them. The OCE asked, "U a real dad or fantasy/rp?" and "chris32033" responded with "Real dad he is 13 you?" The OCE replied that he had a 12 year-old daughter. The OCE questioned "chris32033" as to

whether his son is shy. Kik user "chris32033" responded with "Nah we always been nude together. I'm bit of nudists and when he visits we were always nude started young and very slow." During the conversation, "chris32033" said he engaged in sexual intercourse with his purported son's friends who were also minors. The OCE said, "How far have you gone? Looking to kind of know the pace that is normal." Kik user "chris32033" said, "We fuck each other and suck etc and last year his two best friends came a week during the summer I had him."

11. Kik user "chris32033" told the OCE that he does not have custody of his son but that his son visits for two to three weeks in the summer and on certain holidays. Kik user "chris32033" suggested he and his son meet with the OCE and his daughter. Kik user "chris32033" said, "But be hot to hang the four of us bet my boy would love to meet your girl." Kik user "chris32033" told the OCE that he lived in North Carolina. Kik user "chris32033" told the OCE that his son lives in South Carolina and was approximately five hours away from "chris32033." Kik user "chris32033" asked the OCE to "Imagine watching our kids fucking." In reply, the OCE explained that he and his daughter may be able to meet up with "chris32033" and his son. Kik user "chris32033" made several suggestions regarding the type of lodging and specifically said it should

be remote stating "Gotcha I'm down for whatever but we can be more nude and open in a house or cabin then hotel room." Kik user "chris32033" and the OCE discussed the sexual activities they would want to perform with their purported children. Kik user "chris32033" told the OCE, "She prob would like mine I'm sure lol", referring to his son and the OCE's daughter. When the OCE asked "chris32033", "Think he'd be into it?", "chris32033" responded, "Oh I'm sure he would. He loves to fuck I mean he fucks his gf with his buddies." The OCE replied, "He'd have to be nice bc she hasn't ever been fucked." Kik user "chris32033" later asked the OCE, "I know but what would you want to happen after seeing my boys cock slide in and out of her tight virgin pussy. You get naked and jerk, or you get behind my boy and slide your dad cock in his smooth hole." The OCE asked "chris32033" for a picture of his son that he could show his daughter. Kik user "chris32033" sent the OCE an image of a young white male whose appearance is consistent with a 13 year old. At 3:51 p.m., after the OCE and "chris32033" exchanged a few more messages, the Kik private message was terminated.

12. On April 16, 2020 at 12:04 p.m., the OCE interacted with "chris32033" on Kik again via private message. Kik user "chris32033" asked if the OCE showed his son's image to the OCE's daughter. Kik user "chris32033"

asked for a photo of the OCE's daughter. The OCE sent an image that was not an actual child. Kik user "chris32033" said he sent the image to his purported son, Payton, who expressed an interest in having sex with the OCE's daughter.

13. The OCE asked if "chris32033" had any videos in his collection but did not indicate the videos should contain children or pornography. The OCE indicated "chris32033" should not just search the internet for videos. Kik user "chris32033" said he "mostly have boys stuff" and he subsequently sent three videos to the OCE. The children in all three videos were clearly minors that were engaged in sexual conduct as defined by statute. The OCE questioned how "chris32033" received the videos and "chris32033" replied, "someone sent them to me."

14. On April 16, 2020, an administrative subpoena was issued to Kik for subscriber information for user "chris32033." In response to the subpoena, Kik provided the following:

First name:	Chris
Last Name:	h
Email:	chris32033@yahoo.com (unconfirmed)
Registration	Timestamp: 01/20/2013 at 09:17 p.m.
Device:	iPhone

15. Kik IP address records logged user "chris32033" using the IP address 104.188.162.252 eight times on April 15, 2020 between 1:30 p.m. and



3:51 p.m. A query of the American Registry for Internet Numbers ("ARIN") online database revealed IP address 104.188.162.252 as being registered to AT&T Internet Services.

16. On May 20, 2020, an administrative subpoena was issued to AT&T Internet Services for account subscriber information associated with IP address 104.188.162.252. As a result of the subpoena, AT&T Internet Services, provided the following account information:

Subscriber Name:	Chauncey Brummell
Subscriber Address:	3015 E Wendover Avenue, Greensboro, North Carolina 27405
Email:	chaunceybrummell@gmail.com

17. The AT&T Internet Services, records indicate that IP address 104.188.162.252 was assigned to the account of Chauncey Brummell, residing at 3015 E Wendover Avenue, Greensboro, North Carolina 27405, from March 30, 2020 to April 30, 2020.

18. A check of publicly available databases show Chauncey Brummell, date of birth 04/19/1979, and HALL, date of birth 03/27/1985, as living at 3015 E Wendover Avenue, Greensboro, North Carolina 27405. On May 21, 2020, I observed two vehicles at 3015 E Wendover Avenue, Greensboro, North Carolina 27405, one of which was registered to HALL. Another vehicle at the residence was registered to Chauncey Brummell.

19. Upon receipt of this information, an FBI analyst used available open source databases to identify HALL as a visual arts teacher at Gate City Charter Academy in Greensboro, North Carolina. HALL also manages a photography and graphic design business. The associated business card listed the email address for the business as chris32033@yahoo.com. HALL appears to use the moniker "chris32033" for multiple other social media pages such as Pinterest and Shutterbug. The Facebook page for HALL contains the same black and white photograph, of a middle-aged white male with dark hair, used in the Kik user "chris32033" account.

20. On May 19, 2020, I reviewed the three videos "chris32033" sent to the OCE over Kik Messenger. The following is a brief description of the three videos:

- i. "IMG\_0325" is an MP4 lasting 46 seconds long and depicts a young child's room with a bed and desk. There is a picture on the wall in a different language other than English, perhaps Arabic. A prepubescent male child about the age of 5 years old is lying facedown on the bed wearing a grey hoodie and no pants. A post-pubescent male about the age of 16 years old wearing black glasses and a red and black shirt

enters the video frame. His black pants are pulled down exposing what appears to be an erect penis. He then penetrates the child anally with his penis. The child appears to be in distress as he smothers his face in the pillow and also hits the pillow with his fist multiple times. Based on my training and experience, this video can be classified as Bondage, Discipline, Sadism, and Masochism (BDSM).

- ii. "IMG\_0326" is an MP4 one minute and 58 seconds long and depicts a room with white walls, a desk chair, and a red sofa in the background. Another person (unknown age as only the arm is seen) is on the sofa playing with the sofa pillows. A prepubescent female child about the age of six years old with brown hair is nude lying on top of a nude uncircumcised adult male. The child is using her mouth and hands to provide sexual pleasure to the adult male. The child's eyes are wide, and she appears to be tired and pulls the penis out of her mouth to breathe a few times.
- iii. "IMG\_0327" is an MP4 lasting 37 seconds and depicts a prepubescent male about the age of five years old asleep or

otherwise unconscious and wearing a black shirt or pajamas with an orange zipper. An adult male with what appears to be an erect penis uses his left hand to masturbate on the child's face and penetrates the child's mouth with the tip of the penis. The adult male is using his hand to move his penis and stimulate his penis. The child never appears to awaken.

21. On May 27, 2020, I received a National Center for Missing and Exploited Children (NCMEC) CyberTipline Report from Greensboro Police Department Detective Brandon S. Hilton. The report, generated by Kik on Kik user "chris32033", disclosed that on March 24, 2020, Kik user "chris32033" uploaded and shared two videos and one photo in a Kik messaging group and to another Kik user via private chat message. The children in the two videos and photo were clearly minors that were engaged in sexual conduct as defined by statute.

22. I reviewed the two videos and photo that Kik user "chris32033" uploaded and shared in a Kik messaging group and to another Kik user via private chat message. The following is a brief description of the two videos and a photograph:

- i. A video entitled "13f07a56-646a-44d8-b26d-72e459d84fb3" is an MP4 lasting approximately 41 seconds long and depicts a bathroom with beige colored tile on the wall, a large mirror on the wall reflecting a small window (possibly at night as there is no visible light), and a vanity with toiletry items and hanging towels. A pre-pubescent male child about the age of 6 or 7 years old is standing and facing the camera. The child is wearing a gray t-shirt and no pants. A sound of water running can be heard in the background. The child raises his t-shirt with his left hand and moves his right hand above his penis. He then drops both hands by his side and moves towards the camera to reposition himself. He stands on an unidentified object so his penis is in the center of the camera. He raises his t-shirt with his left hand and pushes his penis between his legs. His penis appears to become erect. He then pushes what appears to be an erect penis between his legs. A voice is heard in the background, in a language other than English, and the child responds while appearing to end the video.

- ii. A photograph entitled "55af9296-2554-41a9-a489-27e2bfebf964" is a JPEG image that depicts water, such as a river or lake, and tall grass. There are trees in the distant background. A pre-pubescent male child about the age of 8 or 9 is sitting on a metal railing by the water, facing the camera, wearing a bracelet on his right wrist and no clothing. The child's skin is lighter in the area where shorts would typically cover the body (an indicator of a suntan). The child is using his hands and feet to support himself on the railing, and his penis is visible.
- iii. A video entitled "6bc4fcd6-6ce6-4243-9753-c3864333e296" is an MP4 lasting approximately 14 seconds long and depicts a pre-pubescent male child about the age of 8 or 9 in a white bathtub, full of water, with white tile on the wall. Toiletries are visible on the side of the bathtub. The walls are dark blue in color, and there is a large window with blinds near the bathtub. The child appears to have braces. He is wearing no clothing and his hair is wet. The child leans back and what appears to be his erect penis is visible

outside of the water. The child stands up and places his penis in the view of the camera.

23. On May 28, 2020, I interviewed Chauncey Brummell at his residence at 3015 E Wendover Avenue, Greensboro, North Carolina 27405. He confirmed he was the subscriber for the AT&T internet service at the residence he has shared with HALL many years. Brummell denied any involvement in the sexual exploitation of children and denied any knowledge of HALL sexually exploiting children.

24. On May 28, 2020, I interviewed HALL at his residence at 3015 E Wendover Avenue, Greensboro, North Carolina 27405. HALL confirmed that he had a Kik account with the username "chris32033" (HALL admitted to chatting with the Kik username, belonging to the OCE, via Kik private messenger). HALL explained that the [OCE] Kik user wanted to meet HALL at a hotel with their purported children. HALL told the [OCE] Kik user that he had a son, even though he did not have children. The [OCE] Kik user wanted HALL's son to take his 12 year old daughter's virginity.

25. When I asked HALL to further describe the three videos that he sent to the [OCE] Kik user, HALL advised that he sent three videos of boys that he found on Kik chat groups. He did not ever download the videos, but

he shared them via Kik private message to the [OCE] Kik user. The first video included a boy who was about 12 or 13 years of age. HALL did not remember what the child was doing in the video. The second video included two boys having sex and the third video included two boys, one boy "jerked off" while the other boy sat on top of him. HALL clarified that he used the term "jerked off" to describe masturbation. According to HALL, the acts described in the videos and the age of the individuals in the videos were definitely inappropriate. He knew it was illegal to share these videos.

26. I showed HALL a screen shot (with genitalia redacted) of the video ("6bc4fcd6-6ce6-4243-9753-c3864333e296") that Kik user "chris32033" uploaded and shared in a Kik messaging group and to another Kik user via private chat message. HALL explained that he found the video from Kik or Mega and shared it on Kik.

27. I showed HALL a photo (with genitalia redacted) of the photo ("55af9296-2554-41a9-a489-27e2bfebf964") that Kik user "chris32033" uploaded and shared in a Kik messaging group and to another Kik user via private chat message. HALL explained that he did not take the photo. He found it Kik. He believed that he was every parent's worst nightmare and that his family will be disappointed in him.



28. HALL chatted with young boys of all different races who he believed were around 14 and 15 years of age, through Kik and Snapchat, on his iPhone. He confirmed their identity through live pictures. He requested that the boys send him a picture of themselves holding a peace sign by their face. He sent the boys nude photos and videos of himself "jerking off", and he received nude photos and videos of the boys "jerking off". After HALL found out some of the boys that he communicated with were underage, he continued contacting them and requesting pictures and videos from them. Most of the chats were random encounters, but HALL repeated communications with some of the boys, in what he described as being like an online relationship.

29. On June 23, 2020, I notified Gate City Charter Academy of the federal and state investigation and arrest of Christopher HALL on multiple state charges for the sexual exploitation of a minor. HALL was employed by Gate City Charter Academy from August 1, 2016 to the day of his resignation on June 16, 2020. On June 24, 2020, Gate City Charter Academy advised they have HALL's work laptop ("SUBJECT'S WORK LAPTOP"), an HP laptop computer, model number 440 G3, serial number 5CD626JP8, which could potentially have evidence regarding the federal and state investigation. Therefore, I am requesting this search warrant to obtain the SUBJECT'S

WORK LAPTOP and search the SUBJECT'S WORK LAPTOP for contraband and evidence, fruits, and instrumentalities of violations of Title 18 U.S.C. §§2252A(a)(2)(A) and 2252A(a)(5)(B) that may be presently located on the SUBJECT'S WORK LAPTOP.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE INTERNET**

30. I have had both training and experience in the investigation of computer-related crimes, as well as that of other agents assisting in the investigation. Based on my training, experience, and knowledge, I know the following:

a. Computers and digital technology are the primary way in which individuals interested in child pornography interact with each other. Computers basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Digital cameras and computers with cameras save photographs or videos as a digital file that can be directly transferred to a computer by connecting the camera or smartphone to the computer, using a cable or via wireless connections such as "WiFi" or "Bluetooth." Photos and videos taken on a digital camera or smartphone may be

stored on a removable memory card in the camera or smartphone. These memory cards are often large enough to store thousands of high-resolution photographs or videos.

c. A device known as a modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Mobile devices such as smartphones and tablet computers may also connect to other computers via wireless connections. Electronic contact can be made to literally millions of computers around the world. Child pornography can therefore be easily, inexpensively and anonymously (through electronic communications) produced, distributed, and received by anyone with access to a computer or smartphone.

d. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. Electronic storage media of various types - to include computer hard drives, external hard drives, CDs, DVDs, and "thumb," "jump," or "flash" drives, which are very small devices that are plugged into a port on the computer - can store thousands of images or videos at very high resolution. It is extremely easy for an individual to take a photo or a video with a digital

camera or camera-bearing smartphone, upload that photo or video to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices. Some media storage devices can easily be concealed and carried on an individual's person. Smartphones and/or mobile phones are also often carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography. Some online services allow a user to set up an account with a remote computing service that may provide email services and/or electronic storage of computer files in any variety of formats. A user can set up an online storage account (sometimes referred to as "cloud" storage) from any computer or smartphone with access to the Internet. Such an account can also be accessed in the same way. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer, smartphone, or external media in most cases.

g. A growing phenomenon related to smartphones and other mobile computing devices is the use of mobile applications, also referred to as “apps.” Apps consist of software downloaded onto mobile devices that enable users to perform a variety of tasks – such as engaging in online chat, sharing digital files, reading a book, or playing a game – on a mobile device. Individuals commonly use such apps to receive, store, distribute, and advertise child pornography, to interact directly with other like-minded offenders or with potential minor victims, and to access cloud-storage services where child pornography may be stored

h. As is the case with most digital technology, communications by way of computer can be saved or stored on the computer used for these purposes. Storing this information can be intentional (*i.e.*, by saving an email as a file on the computer or saving the location of one’s favorite websites in, for example, “bookmarked” files) or unintentional. Digital information, such as the traces of the path of an electronic communication, may also be automatically stored in many places (*e.g.*, temporary files or ISP client software, among others). In addition to electronic communications, a computer user’s Internet activities generally leave traces or “footprints” in the web cache and history files

of the browser used. Such information is often maintained indefinitely until overwritten by other data.

i. Individuals involved in the receipt, possession, and/or distribution of child pornography very frequently possess multiple devices that contain evidence of their interaction with child pornography and/or sexual interest in minors. In modern American culture, most individuals possess multiple devices that have the ability to connect to the Internet (e.g., tablets, desktop computers, laptop computers, and mobile phones). Many individuals also keep prior versions of their devices (e.g., prior cell phones and prior computers). This is the case because (1) individuals are often reluctant to discard devices that frequently contain significant personal information and (2) current devices may malfunction and prior versions can often be used until the current device is repaired or replaced.

#### **SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS**

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT'S WORK LAPTOP, in whatever form they are found. One form in which the records are likely to be found is data stored on a computer's hard drive or other

storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. I submit that since the SUBJECT'S WORK LAPTOP was issued by HALL'S employer to be used by HALL, there is probable cause to believe records referenced above will be stored on that computer or storage medium, for at least the following reasons:

a. Deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

b. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a

computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence



that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on SUBJECT'S WORK LAPTOP because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, email programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. Information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why,

when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, Internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, computers typically contain information that logs: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed

networks and the Internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., Internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping"

program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to

establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

g. I know that individuals who own smartphones often utilize their computer to access files on their smartphones or backup their smartphones to their computers. As HALL confessed to accessing child

pornography on his smartphone, an iPhone XR, the potential exists that HALL used his work laptop to backup his iPhone or used his work laptop to access child pornography.

### CONCLUSION

34. Based on the foregoing, there is probable cause to believe that the federal criminal statutes cited herein have been violated, and that the contraband, property, evidence, fruits and instrumentalities of these offenses, more fully described in Attachment B, are located on the SUBJECT'S WORK LAPTOP, more fully described in Attachment A. I, therefore, respectfully request that the attached warrant be issued authorizing the search of the SUBJECT'S WORK LAPTOP and the seizure of the items listed in Attachment B.

/S/ Emily R. Keller  
Special Agent  
Federal Bureau of Investigations

Sworn and subscribed before me this 30th day of June, 2020.

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on this 30th day of June, 2020, at 3:00p.m.

A handwritten signature in black ink, appearing to read "Joe L. Webster", written over a horizontal line.

Joe L. Webster  
United States Magistrate Judge

**ATTACHMENT A**

**Property to Be Obtained and Searched**

This warrant applies to records and other information related to Christopher HALL'S HP laptop computer, model number 440 G3, serial number 5CD626JP8 ("SUBJECT'S WORK LAPTOP"), which is stored at Gate City Charter Academy, a charter school in Guilford County, located at 123 Flemingfield Road, Greensboro, North Carolina 27405. The SUBJECT'S WORK LAPTOP was issued to HALL by Gate City Charter Academy to conduct work related matters.



## **ATTACHMENT B**

### **ITEMS TO BE SEIZED**

The following materials, which constitute evidence of the commission of a criminal offense, contraband, the fruits of crime, or property designed or intended for use or which is or has been used as the means of committing a criminal offense, namely violations of 18 U.S.C. §§ 2252A(a)(2)(A) and 2252A(a)(5)(B):

1. HP laptop computer, model number 440 G3, serial number 5CD626JP8 (SUBJECT'S WORK LAPTOP), that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.
2. Records, information, and items relating to violations of the statutes described above in the form of:
  - a. Records and information referencing child pornography, as defined in 18 U.S.C. 2256(8), and/or child erotica;
  - b. Records, information, and items referencing or revealing the occupancy or ownership of 3015 E Wendover Avenue, Greensboro, North Carolina 27405, including utility and telephone bills, mail envelopes, or addressed correspondence;
  - c. Records and information referencing or revealing access to and/or use of Kik Messenger;
  - d. Records and information referencing or revealing the use of the handle "chris32033", or any variant thereof, and the identity of the user;

- e. Records and information referencing or revealing the owner or user of an iPhone at 3015 E Wendover Avenue, Greensboro, North Carolina 27405;
  - f. Records and information referencing or revealing the trafficking, advertising, or possession of child pornography, to include the identity of the individuals involved and location of occurrence;
  - g. Records and information referencing or revealing a sexual interest in children or the sexual exploitation of children, to include the identity of the individuals involved and location of occurrence such as social media sites or applications containing groups or chat rooms dedicated to accessing child pornography, to include Kik, Facebook, Tumblr, and Shutterbug as well as online repositories known to be accessed with the intent to view child pornography such as Imjur and TOR;
  - h. Records and information referencing or revealing the use of remote computing services such as email, cloud storage, or online social media services; and
  - i. Records and information referencing minors and/or revealing their identities.
3. For the SUBJECT'S WORK LAPTOP whose seizure is otherwise authorized by this warrant:
- a. Evidence of who used, owned, or controlled the SUBJECT'S WORK LAPTOP at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

- b. Evidence of how and when the SUBJECT'S WORK LAPTOP was used to create, edit, delete, view, or otherwise interact with or access child pornography or share child pornography with others;
- c. Evidence of the attachment to the SUBJECT'S WORK LAPTOP of other storage devices or similar containers for electronic evidence;
- d. Evidence of the Internet Protocol addresses used by the SUBJECT'S WORK LAPTOP;
- e. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT'S WORK LAPTOP;
- f. Documentation and manuals that may be necessary to access the SUBJECT'S WORK LAPTOP or to conduct a forensic examination of the SUBJECT'S WORK LAPTOP;
- g. Evidence of software that would allow others to control the SUBJECT'S WORK LAPTOP, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- h. Evidence of the lack of such malicious software; and
- i. Evidence of programs (and associated data) that are designed to eliminate data from the SUBJECT'S WORK LAPTOP.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data).

The term "storage medium" includes any physical object upon which computer data can be recorded, including external and internal hard drives,

flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact discs, magnetic tapes, memory cards, memory chips, and other magnetic or optical media.